目　　次

第３部　午後問題のテーマ別対策と必要知識

情報処理安全確保支援士制度と試験についての情報

●2016 年 6 月 27 日
　独立行政法人 情報処理推進機構（IPA）は「“情報処理安全確保支援士”と現行の情報セキュリティスペシャリスト試験の位置付けについて」を公表しました。その（3）制度の詳細には，

「支援士試験の受験手数料，登録手数料，更新に必要な講習などの詳細は，2016 年 10 月末を目途に決定される予定です」

と記載されています。

●2016 年 9 月 7 日
　経済産業省は「情報処理の促進に関する法律施行令の一部を改正する政令案に対する意見の募集（パブリックコメント）について」を公表しました。

●2016 年 9 月 8 日
　経済産業省は「情報処理の促進に関する法律施行令の一部を改正する政令案等に対する意見公募要領」を公表しました。

◆情報処理安全確保支援士制度と試験についての情報，内容については，常に IPA のホームページ（http://www.jitec.ipa.go.jp/）などで確認するようにしてください。

独立行政法人 情報処理推進機構のプレスリリース (2016 年 6 月 27 日)

“情報処理安全確保支援士”と現行の情報セキュリティスペシャリスト試験の位置付けについて
～情報セキュリティスペシャリスト試験の合格者は支援士への有資格者に～

IPA（独立行政法人情報処理推進機構，理事長：富田 達夫）は，情報処理安全確保支援士制度が創設されることを踏まえ，情報処理安全確保支援士と現行の情報処理技術者試験「情報セキュリティスペシャリスト試験」の位置付け，試験実施予定などについて公表しました。

経済産業省は 2016 年 4 月 27 日に，国家資格となる「情報処理安全確保支援士」制度を 2016 年度内に新たに創設するとともに，「情報処理安全確保支援士試験（以下，支援士試験)」を 2017 年度から実施することを公表しました(*1)。

同制度は情報セキュリティの専門的な知識・技能を有する専門人材を登録・公表するもので，支援士試験は，現在実施している国家試験「情報処理技術者試験」の「情報セキュリティスペシャリスト試験（以下，SC 試験)」の内容をベースに実施されます。

試験制度における両試験の位置付けは下図のとおりで，これまで情報処理技術者試験制度の枠組みの中で実施してきた SC 試験は廃止され，支援士試験制度の中で実施するとされています。

(*1) 試験ワーキンググループ中間とりまめ ～ 情報処理安全確保支援士制度～
http://www.meti.go.jp/committee/sankoushin/shojo/johokeizai/shiken_wg/pdf/report_01_01_00.pdf

Part 1　第2章　Chapter 2

情報処理安全確保支援士試験の対策

第2章「情報処理安全確保支援士試験の対策」は，情報セキュリティスペシャリスト試験の対策に基づいて説明しています。情報処理安全確保支援士制度の詳細が決定された段階で，アイテックホームページに「追加・補足情報」を掲載していく予定です。詳しくは，P.15 を参照してください。

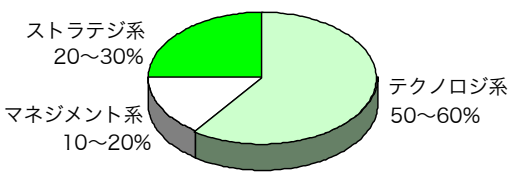
なお，IPA のホームページには，「支援士試験の受験手数料，登録手数料，更新に必要な講習などの詳細は，2016 年 10 月末を目途に決定される予定です」と掲載されています（2016 年 8 月現在）。

学習の開始が遅れないように，10 月末に情報処理安全確保支援士試験の内容が決定されるまでに，できることはしておきましょう。特に，過去に SC 試験を受験したことのない人は，早めの対策が不可欠ですからね。

ただし，ここで説明する試験対策はあくまでも暫定版です。情報処理安全確保支援士試験の内容が発表された段階で，アイテックホームページも更新しますので，必ず目を通してください。

1.　午前Ⅰ対策

SC 試験の午前Ⅰ試験は，情報処理技術者試験の全範囲を対象とした高度系 9 区分共通の試験でした。30 問のすべての問題が，応用情報技術者試験の午前問題から抜粋されています。応用情報技術者試験の午前問題は全部で 80 問なので，そこから 4 割弱の問題が使われていることになります。配分は，テクノロジ系が過半数を占めています。難易度は（午前Ⅱ以後の“レベル 4”よりも 1 段階低い）“レベル 3”相当になります。つまり，それほど難しい問題は出題されませんが，非常に幅広い知識が必要でした。



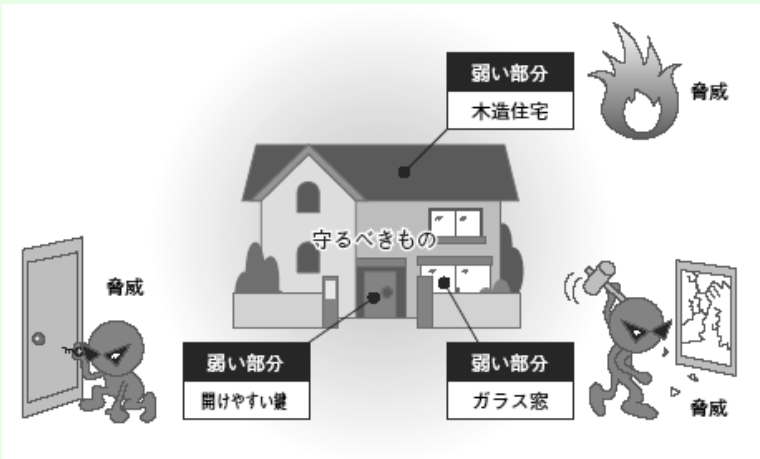
図表 1-2-1　分野別出題比率

1　情報セキュリティの概念

情報セキュリティの全体像を理解する

セキュリティは，通常，図に見られるように，次の三つの要素が存在するときに必要になると言われています。

① 守るべきものの存在
② それを脅かす存在（脅威）
③ その脅威が突いてくる弱い部分の存在



図表 2-1-1　セキュリティを考えるときの三つの要素のイメージ（例）

図表 2-1-1 は，一般的なセキュリティの概念になりますが，企業が情報セキュリティを考えるとき，この三つの要素は，それぞれ次のような名称で呼ばれます。まずは，この三つの名称を覚えるところからスタートしましょう。

4　脅威

情報を詐取したり，改ざんや破壊したりする目的で，システムに対する攻撃が行われます。マルウェア，不正アクセス，盗聴，なりすまし，サービス不能攻撃，アプリケーションへの攻撃など。個々の攻撃手法には，独特の名称が付けられているので，それを覚えていきましょう。

(1)　マルウェア（malware）

悪意のコード（malicious code），又は悪意のソフトウェア（malicious software）の総称。コンピュータウイルス（ワーム，トロイの木馬，ボット等）に加えて，バックドアやルートキット，キーロガーなどの攻撃ツール，スパイウェアなども含んだ概念になります。

代表的なマルウェア		概要
ウイルス		自己伝染機能，潜伏機能，発病機能のいずれか一つ以上を有するもの（経済産業省：コンピュータウイルス基準より）。
	ワーム	ネットワークを通じてほかのコンピュータに拡散することを目的とした不正プログラム。
	トロイの木馬	増殖が主目的ではなく，ひっそりと常駐し，特定の日時や外部からの指示で破壊活動を開始する。
	ボット	コンピュータウイルスやワームの一種。語源はロボット。ボットを仕掛けた攻撃者は，遠隔操作によって，その端末から迷惑メールを送信したり，他のコンピュータを攻撃したりする。同一の指令サーバ配下のボットで形成されたネットワークをボットネットという。
攻撃ツール	バックドア	裏口。ハッキング成功時に，次回からアクセスや操作をしやすいように常駐させておくプログラムなど。
	ルートキット（rootkit）	様々なハッキングツールをまとめてキット状にしたもの。不正プログラムそのものや，バックドアの設置，ログの改ざんなど，標的サーバに不正侵入した後に使うツールなどをまとめたもの。
	キーロガー	打鍵したキーの使用を記録するソフト。
スパイウェア		利用者のコンピュータ内部の情報（環境設定情報，アクセス履歴など）を外部に自動的に通知する目的で常駐するプログラム（ソフトウェア）。

暗記事項

暗記事項をまとめました。しっかりと暗記してください。

問題	解答
1．情報セキュリティの概念	
三大要素（3）	① 情報資産 ② 脅威 ③ 脆弱性
情報セキュリティ確保の手順（4）	① 基本方針，情報セキュリティ委員会設置 ② 情報セキュリティポリシの作成 ③ セキュリティ教育，周知活動 ④ 定期的に評価・監査，必要に応じて見直し
情報セキュリティ対策（4）	① 抑止効果を狙う ② 予防的対策 ③ 事後対策（検知，復旧） ④ 再発防止策
情報セキュリティの三要素（3）	① Confidentiality；機密性 ② Integrity；完全性 ③ Availability；可用性
2．情報セキュリティマネジメント	
制度（6）	① 情報セキュリティマネジメント試験（新設） ② ISMS 適合性評価制度 ③ システム監査制度 ④ 情報セキュリティ監査制度 ⑤ プライバシーマーク制度 ⑥ 内部統制制度
情報セキュリティの推進体制（3）	① 情報セキュリティ推進組織 ② CISO ③ 情報セキュリティ管理者
ISMS 構築手順（10）	① ISMS の適用範囲を定義 ② ISMS の基本方針を定義 ③ リスクアセスメントの取組方法を定義 ④ リスク特定 ⑤ リスク分析・リスク評価 ⑥ リスク対応 ⑦ 管理目的と管理策を選択 ⑧ 残留リスクの承認 ⑨ ISMS の導入・運用を許可 ⑩ 適用宣言書を作成

Part 3　第１章　Chapter 1

認証とアクセスコントロール

認証とアクセスコントロールに関する問題は，過去の頻出分野の一つになります。意外かもしれませんが，その中でも，利用者 ID やパスワードの適切な運用に関する設問が案外多いのをご存知でしょうか。内容を少し見てもらえれば明白ですが，この分野は，セキュリティの厳しい会社では，自分が守る立場で関与していることもあるため，日ごろから“情報セキュリティを守ろうと意識の高い人”なら，その観点でも十分に点数を取ることができるところです。まずはここから押さえていきましょう。この傾向は，情報処理安全確保支援士試験でも継続される可能性が高いと予測できますからね。

もちろん，利用者 ID とパスワードの運用を知っているだけで十分だとは言えません。認証と権限そのものについて理解するとともに，認証技術として，シングルサインオンや，バイオメトリクス認証，IEEE 802.1X 認証などについての知識も必要になります。まとめてここで学習しましょう。

●学習目標　（次の知識が，瞬時に“アウトプット”できるようになる）

(1)　識別，認証，権限（の違い）
(2)　アクセスコントロールの種類（DAC，MAC，RBAC の違い）
(3)　アクセス権付与の原則
(4)　特権。特権ユーザ，特権 ID
(5)　アカウント（利用者 ID）の適切な運用管理方法
(6)　パスワードの適切な運用管理方法
(7)　パスワードの暗号化
(8)　ワンタイムパスワード
(9)　バイオメトリクス認証
(10) IEEE 802.1X 認証
　①　EAP（EAP-MD5，PEAP，EAP-TLS の違い）
　②　RADIUS
　③　検疫ネットワーク（認証シーケンス）
(11) リスクベース認証
(12) シングルサインオン

1．過去の出題内容を確認

出現率 73%

PKIは暗号技術などと同じようにセキュリティのインフラなので，午後問題にメインで出題されることは少ないですが，ごくごく普通に使われているので，逆に，しっかりとした知識が必要になるテーマになります。

そんなPKIの過去問題ですが，一番軸になる問題は，SC試験のH21年春午後Ⅱ問1だと考えています。この問題のキーワードは，「CP/CPS」，「自営CA」，「商用CA」，「ルートCA」，「CSR」，「鍵管理のアプライアンス製品」などです。

他には，H23年秋午後Ⅰ問3でプロキシ経由のWebアクセスをテーマにした問題が出題されています。このときのキーワードは「プロキシによるSSLの内容検査」，「コモンネーム」ですね。古くは，SU試験開始直後のH13年，H14年に出題されています。H13年午後Ⅰ問3「電子商取引の情報セキュリティ対策」では基礎的な問題が，H14年午後Ⅰ問2「認証システム」では，公開鍵証明書（ディジタル証明書）の更新のタイミングなどが問われています。

表　全出題実績

試験＼期		平成21年春	平成21年秋	平成22年春	平成22年秋	平成23年春	平成23年秋	平成24年春	平成24年秋	平成25年春	平成25年秋
SC	午後Ⅰ	－－－－	○－△－	－－○－	△－○－	－－－－	－－◎－	－－－－	○－－○	－－－－	－－－－
	午後Ⅱ	◎－＼	－△＼	－－＼	－－＼	－△＼	△△＼	－－＼	○－＼	－－＼	－△＼

試験＼期		平成26年春	平成26年秋	平成27年春	平成27年秋	平成28年春
SC	午後Ⅰ	－－○	－◎－	○－－	－－－	－△◎
	午後Ⅱ	－－＼	△○＼	－○＼	○－＼	－－＼

試験＼春期		平成18年	平成19年	平成20年
SV	午後Ⅰ	－△○○	－－－○	－－△－
	午後Ⅱ	－○＼	－－＼	－△＼

試験＼秋期		平成13年	平成14年	平成15年	平成16年	平成17年	平成18年	平成19年	平成20年
SU(SS)	午後Ⅰ	－－◎－	－◎○－	－－－－	－－－－	－－－◎	－－－－	○－－－	－－－○
	午後Ⅱ	－－＼	－－＼	－－＼	－－＼	○－＼	－－＼	－－＼	－○＼

※1.記号の意味(◎＝メインテーマとして出題，○＝設問単位の出題，△＝問題文に登場，－＝無関係)
※2.各期内の欄は，左から順に問1，問2，問3，問4を表しています。

２．学習方法

本章の具体的な学習方法と学習手順を下記①～⑥に，また，③，④，⑤で使用する過去問題を図表 3-5-1 に，それぞれまとめました。章末の演習問題を，時間を計測して解くかどうかは，情報処理安全確保支援士試験の形式次第ですが，それ以外の部分は，この学習方法で大丈夫です。

試験区分	出題年度 期	問	タイトル	キーワード	本書掲載
(SW) AP	平成19年春	午後Ⅰ問1	ファイアウォールによるアクセス制御	FWの基礎	DL(※)
	平成21年春	午後　問9	ファイアウォールの設定	FWの基礎	DL(※)
SV	平成19年春	午後Ⅰ問2	ネットワークのセキュリティ	FW，IDS，IPSの基礎	DL(※)
SC	平成25年春	午後Ⅰ問2	IPアドレス詐称対策	FWのIPアドレス詐称対策機能	DL(※)
	平成27年秋	午後Ⅰ問1	ソフトウェアの脆弱性への対応	WAF	P.272

(※)＝https://www.jitec.ipa.go.jp/1_04hanni_sukiru/_index_mondai.html からダウンロード

Check Box **図表 3-5-1　この章のテーマに関連する過去問題（FE，AP，SU，SV，SC）**

□ ① 前提知識の確認

ネットワーク分野の IP ネットワークやルータの基礎知識が必要です。

□ ② 本章の知識の確認

続いて，本章の「5．ファイアウォール・IDS・IPS・UTM に関する知識の整理」を熟読しましょう。

□ ③ レベル２（FE），レベル３（AP）の過去問題で理解を深める

図表 3-5-1 の AP（SW）区分の 2 問に目を通しておきましょう。いずれもファイアウォールに関する基礎の問題で，問題と解答例だけで十分理解できます（問題と解答例は試験センターのサイトからダウンロードできます）。

□ ④ レベル４（SU，SV，SC）の過去問題で理解を深める

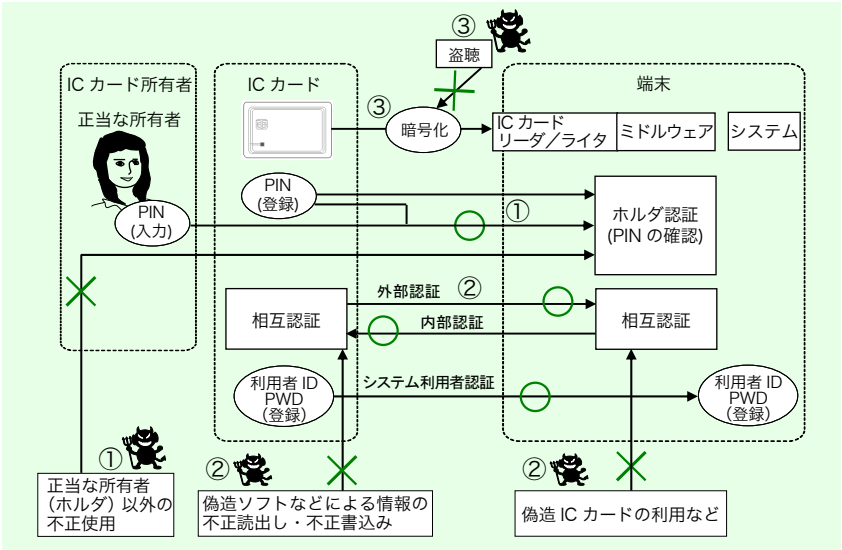
続いて，平成 19 年春の SV（テクニカルエンジニア情報セキュリティ）の午後Ⅰ問 2 の問題を読みましょう（解く必要はありません）。ファイアウォールに加えて，IDS と IPS の基礎（フォールスポジティブ，フォールスネガティブ）が確認できます。

□ ⑤ 章末の演習問題で確認

①～④で理解が深まれば，章末の「6．演習問題」を解いてみましょう。

６．IC カードに関する知識の整理

IC カードに対する脅威と対策をまとめたものが次の図表になります。こうした全体像の把握は，とても大切です。最初に，この図表を見ながら全体像を把握してみてください。そして，その後，学習目標に従って，最低限必要な知識を整理していきましょう。



図表 3-8-2　IC カードに対する脅威と対策の全体図

	脅威	ICカードのセキュリティ要件	機能	
①	ICカードの不正利用	ICカードが，正当な使用権限をもった者（ホルダ）以外の者に使用されないこと	PINによる所有者本人確認（ホルダ認証）	
②	偽造ICカードの利用	正規のICカードだけが使用できること	端末－ICカード間の相互認証	端末がICカードを認証する（内部認証）
	内容の不正読出しや不正書込み	ICカード内部の情報が不正に読み出されたり，改ざんされたりしないこと		ICカードが端末を認証する（外部認証）
③	盗聴による情報漏洩	リーダとICカードの間の通信が傍受されても，内容が分からないこと	暗号化	

図表 3-8-3　IC カードに対する脅威とセキュリティ要件，及び機能

6．演習問題

(H28 春-SC 午後Ⅱ問 1)

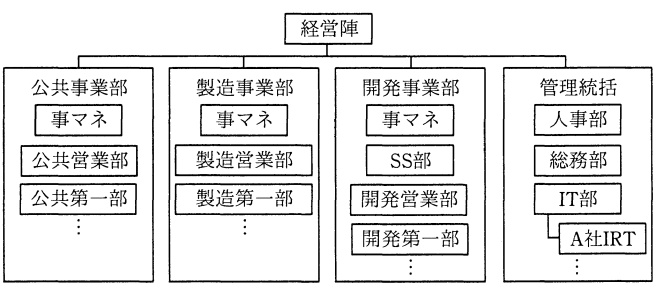
CSIRT 構築とセキュリティ設計に関する次の記述を読んで，設問 1～6 に答えよ。

A 社は，従業員数 3,000 名の独立系ソフトウェア開発会社である。受託開発業務が中心であるが，一部の部署で展開しているサービス事業が拡大傾向にある。

〔A 社の組織〕

A 社には，公共事業部，製造事業部，開発事業部，管理統括の四つの組織がある。公共事業部と製造事業部は，それぞれの業種の顧客システムの開発が事業の中心である。開発事業部には，公共及び製造以外の業種の顧客システムの開発を行う部署と，A 社独自のサービス事業を行う部署とがある。後者のうち，ソリューションサービス部（以下，SS 部という）は，国内の人材をデータベース化し，顧客企業に紹介する Web サービス（以下，高度人材サービスという）を提供している。管理統括は，人事部，総務部，情報システム部（以下，IT 部という）などで構成される。

A 社では，各事業部に事業部マネジメント（以下，事マネという）という組織があり，事業部の実務的な意思決定を行っている。A 社の組織図を図 1 に示す。



注記　“A 社 IRT”は，A 社における CSIRT の呼称である。

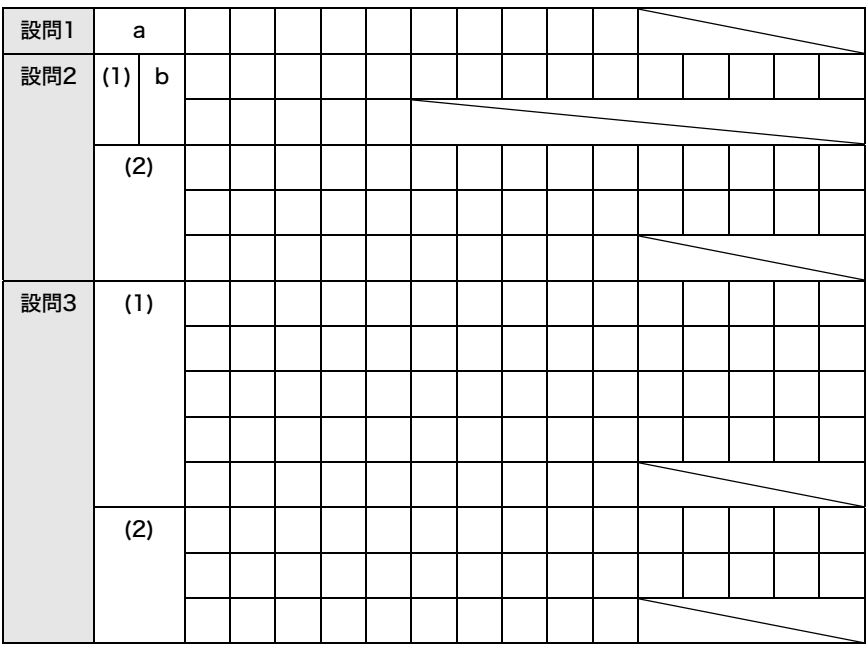
図 1　A 社の組織図

〔A 社のセキュリティポリシ〕

A 社のセキュリティポリシでは，セキュリティインシデント（以下，インシデントという）発生時の対応を図 2 のように定めているが，どのような事象がインシデントに該当するかは定義されていない。インシデントの報告を受け付けた際の，A 社 IRT の運用手順の概要を表 1 に示す。

〔解答用紙〕

コピーして活用してください。また，アイテックホームページ https://www.itec.co.jp/ からダウンロードすることもできます（P.47 参照）。



〔解説〕

本問では，インシデントの発生を契機として，社内に CSIRT（Computer Security Incident Response Team）の専門チームを構成する際に必要となる事項やその目的，脆弱性情報ハンドリングにおいて，各情報機器の構成管理情報を活用することによる効果，各部署との連携方法などに関するものが出題されています。リバースブルートフォース攻撃の検知方法を除き，前提知識が必要な問題はほとんどなく，問題の記述内容に照らし合わせて，丁寧に解答を作成していきます。なお，共通脆弱性評価システム（CVSS）に関する設問がありますが，問題の条件を的確に考慮すれば正解できると思われます。全体の難易度を評価すると，少し易しいレベルといえます。

［設問1］

この設問は，表1（A社 IRT の運用手順（概要））中の空欄 a に入れる，A社 IRT が決定すべきことを，10字以内で答えるものです。そして，空欄 a は，トリアージの「A社 IRT は，受け付けた内容の事実確認を行った上で，あらかじめ定めた基準に従い，重要度や優先度を考慮して，［ a ］を判断する」という作業内容の中にあります。

トリアージ（triage）とは，もともと医療現場において患者の緊急度に応じて適切な処置方法を決定し選別を行うという意味で使用されたものですが，セキュリティ分野においても，ウイルスが侵入するといったセキュリティ上の脅威が発生した際に，復旧作業を行う対策内容やその優先順位を決める作業のことをいうようになりました。また，表1の運用手順では，空欄 a に応じて番号3（調査依頼検討）又は番号6（完了）に進むことになっています。このため，A社 IRT が決定すべきこととしては，報告を受けたインシデントに対する対応を行うかどうか，つまり対応の要否を決める必要があります。したがって，空欄 a には“対応の要否”という字句が入ります。

［設問2］

(1) この設問は，表2（A社 IRT に関する問題点（抜粋））中及び本文中の［ b ］入れる適切な字句を，〔A社 IRT の現状〕の内容を踏まえ，20字以内で答えるものです。

〔A社 IRT の現状〕に「A社の従業員に対して，A社 IRT の存在を積極的には周知しておらず，A社 IRT に報告すべきインシデントの範囲についても明確には定義していない」と記述されています。このため，A社 IRT に関する問題点のうち，明確化すべき事項としては，A社 IRT に報告すべきインシ